The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	NO. CR19-0159 RSL GOVERNMENT'S REPLY IN SUPPORT OF MOTION TO SEAL AND REDACT ADMITTED TRIAL EXHIBITS

The United States of America, by and through Nicholas W. Brown, United States Attorney for the Western District of Washington, and Andrew C. Friedman, Jessica M. Manca, and Tania M. Culbertson, Assistant United States Attorneys for said District, hereby files this Government's Reply in Support of Motion to Seal and Redact Admitted Trial Exhibits.

Thompson does not appear to contest (1) sealing of Exhibits 506 and 731, (2) redaction of PII, consistent with the local rules, and (3) redaction of account numbers, consistent with the local rules (which the Government understands to include its request to redact Amazon account numbers to the last four digits). Dkt. No. 359 at 1. Thompson does contest sealing or redaction of (1) malware scripts, (2) victims' role names, and (3) victims' file structures/lists (except those in Exhibit 731). Thompson's proffered arguments do not support her position.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I. VICTIM INFORMATION

As an initial matter, Thompson's brief addresses only malware scripts. It does not address victims' role names and victims' file structures/lists. Such material is confidential information of Thompson's victims, the publication of which would harm them. Because Thompson offers no argument to the contrary, the Court should hold that this information is entitled to protection from disclosure, and should be sealed or redacted. *See, e.g.*, *FTC v. Qualcomm Inc.*, No. 17-CV-00220-LHK, 2019 U.S. Dist. LEXIS 1289 at *14-15 (N.D. Cal. Jan. 3, 2019). As a result, the Court should grant the Government's motion with respect to exhibits identified as containing victims' role names and victims' file structures/lists.

II. MALWARE SCRIPTS

Thompson does make several arguments as to why her malware scripts should not be sealed or redacted. None is persuasive.

First, Thompson argues that the government has not shown a substantial probability someone else would copy her code. Dkt. No. 359 at 2. But we live in an era of copycat crime. As this Court is no doubt aware, crimes that receive a high degree of publicity often lead to other people committing the same crime. It simply defies belief to think that were Thompson's malware publicly available in the court file of her criminal case, some other person(s) would not look at it and try to copy Thompson's actions.

Second, Thompson argues that her code has "been widely disseminated (and dissected) within the tech community," so that "the cat is already out of the proverbial bag." Dkt. No. 359 at 3. Thompson supports this argument by citing two articles about her crime. Although Thompson's brief provides a link for the first (titled "Case Study: AWS and Capital One, System Weakness"), when the government sought to use that link, it received only a response that the article could not be reached and might be temporarily down or have been moved. The second article (titled "Capital One hack highlights SSRF

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

concerns for AWS"), speculates about Thompson's attack vector, specifically, that Thompson committed a server-side request forgery (SSRF) attack. Significantly, the article does *not* contain scripts that would allow a reader to commit the same hack as Thompson.

Thompson also supports her claim that the cat is out of the bag by citing two sections of Amazon Web Services (AWS) guides that she claims "publicly disclose[] much of the same scripting that Ms. Thompson utilized." Dkt. No. 359 at 3. It is scarcely surprising that Thompson's attack included commands contained in the guides that would be recognized within the AWS computing environment. But the AWS guides to which Thompson points neither contain, nor pull together, the multiple steps that Thompson used to commit her hack. One could not simply read the guides and replicate Thompson's attack. By contrast, a person with Thompson's scripts could do exactly that. As a result, none of the materials to which Thompson cites show that the cat is fully out of the bag.

Third, Thompson argues that AWS already notified its customers of the vulnerability. While it is true that AWS notified customers that it determined had misconfigured web application firewalls in 2019, AWS has millions of customers. It seems inevitable some of those customers either failed to heed AWS' warning, or subsequently misconfigured their firewalls. As a result, a person who scanned the entire universe of AWS customers – as Thompson did, and as her malware scripts would allow others to do – almost certainly would find other victims to attack today.

Significantly, the only benefit that Thompson asserts would result from unsealing her scripts is that doing so supposedly would add clarity to Computer Fraud and Abuse Act (CFAA) law. But it is not necessary to publish Thompson's actual malware to achieve that end. The briefs in the case, the testimony and argument at trial, and the press coverage of the case all make it abundantly clear what Thompson did, and the nature of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the security flaw that she exploited. Seeing the actual computer scripts that Thompson used would not add anything to this understanding. Thompson was perfectly able to make arguments based upon *Van Buren v. United States,* 141 S. Ct. 1648 (2021), and *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), without seeing the computer code and/or commands at issue in those cases. Security researchers, and others, similarly will be able to develop principles and draw lines that may be affected by Thompson's case without reading Thompson's actual malware scripts.

IV. CONCLUSION

For the foregoing reasons, the Court should find that the government has established that sealing or redacting the exhibits identified by the government would serve a compelling interest, and that failure to seal or redact would harm that interest. As a result, the Court should grant the government's motion.

DATED: this 5th day of August, 2022.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

s/ Andrew C. Friedman
s/ Jessica M. Manca
s/ Tania M. Culbertson
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Phone: (206) 553-7970
Fax: (206) 553-0882
Email: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdjo.gov
Tania.Culbertson@usdoj.gov